World Journal of Agriculture and Urbanization
Volume: 01 | January 2022
https://wjau.academicjournal.io/index.php/wjau

Communication Control Systems, Methodology

Usmonov Maxsud Tulqin o'g'li
Tashkent University of Information Technologies Karshi branch 4rd year student

Qodirov Farrux Ergash o'g'li
Ilmiy rahbar

Abstract: *The success of many businesses and organizations today largely depends on the reliability and quality of the network services and applications they use, which in turn depend on the state of the network infrastructure that transmits the traffic to these services and applications. and the parameters are finally affected to a great extent. Monitoring the network, as well as controlling the critical parameters (KPIs) for the efficiency of network services and applications, helps users to quickly identify and troubleshoot problems in their work to maintain the required quality of services provided.*

Keywords: *NetFlow, SPAN-port, Phantom Virtualization Tap, IT (information technology) specialists use a variety of monitoring tools, including protocol analyzers (analyzers), RMON tube instruments (probes), NetFlow miners (collectors), IDS / IPS systems and network.*

1. INTRODUCTION

1. The most optimal connection
2. Network monitoring and analysis systems
3. Control of virtualized environments

Today, the success of many enterprises and organizations depends largely on the reliability and quality of network services and applications they use, which in turn depends on the state and parameters of the network infrastructure that transmits traffic to these services and applications. finally affected to an extent. Monitoring the network, as well as controlling the critical parameters (KPIs) for the effectiveness of network services and applications, helps users to quickly identify and troubleshoot problems in their work to maintain the required quality of services provided. Optimal connection Monitoring the operation of a network and network services and applications involves capturing and analyzing network traffic. This is not only to identify (diagnose) problems in the network, but also to optimize the work of critical services and applications, as well as information security within the framework of the System of Technical Means (SORM) to ensure the functions of operational search activities. in order to identify relevant threats and to legally intercept (capture) information transmitted over the network. IT specialists record various volumes of monitoring tools, including protocol analyzers, RMON tubing devices (probes), NetFlow collectors (collectors), IDS / IPS systems, and large amounts of network traffic. use test tools (probes) based on available server platforms (see section "Analysis, monitoring and detection (diagnostics) of the corporate network"). In order to capture the network traffic that needs to be controlled, it is preferable to use a special network of monitoring devices (a device that divides the network into branches) or disconnectors (switches) that have the functions of such a network to connect them to the network. The Ethernet connector is overloaded and does not transmit defective packets.

2. METHODS

Unlike a possible SPAN port, a router that connects to a network channel outlet allows all traffic (all!) transmitted over that channel to be controlled, regardless of its load level. The router has no effect on the operation of the controlled channel and does not reduce its reliability, because in the event of a power outage, the router relative to the copper line remains transparent for controlled traffic, fiber-optic and the branch is a passive device that does not need to be supplied with electricity at all. In addition, because the monitoring tool connected via the network does not need an IP address, it will be isolated from the network, which will significantly reduce the chances of it being attacked by hackers. On sale there is a very wide range of networkers with different speeds - 10 Mbit / s to 100 Gbit / s, which support the transmission of data for copper or fiber-optic lines. Including the usual branching regenerative networking devices are produced and used when it is necessary to control the same traffic at the same time with the help of several monitoring tools. Such a device outputs networked traffic simultaneously through several of its monitoring ports. If the number of network channels to be monitored exceeds the number of monitoring tools available, an aggregating network can be used, which combines traffic from multiple monitored channels and monitors the aggregated flow on its own or more. outputs through ports. However, the speed of this flow may exceed the bandwidth of the monitoring port, and in this case leads to the unacceptable loss of packets. One way to avoid this is to choose a model of aggregating network that has a large enough buffer. It can also be overloaded when the monitoring device is connected to a faster network channel (for example, if a 1 GE port analyzer is connected to a 10 GE line using a 10 Gigabit router). In order to reduce the load on the monitoring tools, network filtering of primary traffic is widely used, so that the tool provides only the information it needs to perform its basic functions (for example, to detect attacks on the network). takes It is also possible to distribute high-speed traffic almost equally between several monitoring devices with the help of a device with a load balancing function. In this case, the flow of packets is often transmitted it is important that it is stored in its entirety, that is, all packets belonging to the same stream must arrive at the same monitoring medium (in the group of tools that have the same load balancing). Traffic filtering and load balancing can protect investments in existing monitoring tools when higher-speed network technologies are introduced. The functions of traffic aggregation and regeneration, filtering and load balancing are available in the switches of the monitoring devices and in the devices that balance the load on them. Thus, if monitoring devices need to be changed frequently from one channel to another and / or traffic filtering and load balancing functions are required, these tools can be installed directly on routers or SPAN ports. not correct, but must be connected via appropriate breakers. When it is necessary to use a monitoring device (for example, an IPS) connected to the network channel outlet (for example, IPS), a bypass switch should be activated. If this tool fails for any reason, the bypass switch will divert traffic around it, thereby maintaining access to critical services and applications (users). for). In addition to the usual branching and bypass connectors on sale, there are various types of these devices that allow you to view RMON statistics without having to connect a special monitoring device. RMON support is also available on monitoring equipment connectors. Net Optics manufactures a wide range of routers, bypass switches, as well as monitoring tool switches and xBalancer load balancing devices belonging to the Director family. Director devices interrupt, aggregate, regenerate, filter, and evenly distribute the traffic to be monitored by the monitoring tools connected to them. The smartest members of this family ensure that the flow is balanced by changing the load (dynamically) while maintaining the integrity of the traffic, and that the traffic is initially filtered using the DPI function. Unlike the Director connectors, the xBalancer device is able to distribute the load on the inline-monitoring tools evenly (while maintaining the integrity of the flows). In a controlled network Net Optics offers the Indigo Pro management platform to centralize the management of many of its installed products.

Controlling virtualized environments In recent years, there has been a widespread popularization of virtualized network environments that increase the efficiency and flexibility of IT (information technology) systems, as well as reduce costs. However, in the same hypervisor itself, it is not possible to capture and analyze the traffic transmitted between virtual machines with the help of conventional physical monitoring tools. Lack of control over this traffic poses a threat to the information security of the enterprise and makes it difficult to detect (diagnose) network outages. As a solution to this problem, Net Optics offers the use of its own Phantom Virtualization Tap (DT) software designed to control traffic in virtualized computing environments. The Phantom Monitor component, which is installed inside the hypervisor core of this software solution, captures (captures) all traffic transmitted between virtual machines via a virtual switch (switch) and captures captured (captured) packets. mental filtering, as well as sending the data to be monitored. In addition, this component has the ability to send captured (captured) traffic to a physical network port for monitoring using traditional physical monitoring tools. The Phantom Virtualization Tap solution does not interfere with the operation of virtual machines and does not require any modification (change of appearance). The second major software component of this solution, the Phantom Manager, is designed to collect and transmit traffic information, as well as to manage a large number of virtual networkers running on controlled hosts. Statistics on the performance of virtual environments are provided in the second and third stages (number of packets transmitted, loading, etc.). Of course, to monitor the virtualized environment, it is possible to extract traffic from it with the help of SPAN-ports of the virtual connector, but for this purpose up to half of the capacity of this connector is spent. In contrast, the Phantom Virtualization Tap virtual network does not load the virtual connector, and its bandwidth remains unchanged. Phantom Virtualization Tap solution for the most common virtualization tools (platforms): VMware vSphere ESX / ESXi Server 4.x / 5.x; Microsoft Hyper-V 8.x; Citrix Xen Server 5.6.x; Redhat KVM 2.6.32 and Oracle VM 3.0 compatible (compatible). This solution helps to ensure the security and reliability of virtual environments, as well as their compliance with regulatory requirements. It is necessary to prepare for monitoring in advance

Various branching devices, bypass switches (switches) installed in the controlled network in a multi-level network monitoring system and providing easy and convenient connection of various monitoring means to it and the disconnectors of the monitoring tools form an access point (see picture), also known in Net Optics as the Monitoring Access Platform (MAP). This platform transmits the traffic to the monitoring devices (probes) of various types, which in turn provide information on the operation of the network, network services and applications. provides high-level monitoring and management software tools. Net Optics recommends pre-planning the implementation of MAP as part of a future network and installing MAP devices along with other network equipment during its creation. It is a good idea to create a MAP before network problems occur. In the MAP architecture, it is necessary to consider the ability to monitor the traffic of network channels, which are critical at the levels of access, distribution and network core, as well as in the data center (MIM) where the enterprise's servers are located. . Due to the large number of high-speed lines in the Data Center (MIM) and the core of the network, there are devices and aggregators that aggregate multi-port channels belonging to the Director family. it is recommended to install switches. To control virtualized environments, it is advisable to run Phantom Virtualization Tap virtual networking on servers in the data center (MIM).

3. RESULTS

it is important that it is stored in its entirety, that is, all packets belonging to the same stream must arrive at the same monitoring medium (in the group of tools that have the same load balancing). Traffic filtering and load balancing can protect investments in existing monitoring tools when higher-speed network technologies are introduced. The functions of traffic aggregation and

regeneration, filtering and load balancing are available in the switches of the monitoring devices and in the devices that balance the load on them. Thus, if monitoring devices need to be changed frequently from one channel to another and / or traffic filtering and load balancing functions are required, these tools can be installed directly on routers or SPAN ports. not correct, but must be connected via appropriate breakers. When it is necessary to use a monitoring device (for example, an IPS) connected to the network channel outlet (for example, IPS), a bypass switch should be activated. If this tool fails for any reason, the bypass switch will divert traffic around it, thereby maintaining access to critical services and applications (users). for). In addition to the usual branching and bypass connectors on sale, there are various types of these devices that allow you to view RMON statistics without having to connect a special monitoring device. RMON support is also available on monitoring equipment connectors. Net Optics manufactures a wide range of routers, bypass switches, as well as monitoring tool switches and xBalancer load balancing devices belonging to the Director family. Director devices interrupt, aggregate, regenerate, filter, and evenly distribute the traffic to be monitored by the monitoring tools connected to them. The smartest members of this family ensure that the flow is balanced by changing the load (dynamically) while maintaining the integrity of the traffic, and that the traffic is initially filtered using the DPI function. Unlike the Director connectors, the xBalancer device is able to distribute the load on the inline-monitoring tools evenly (while maintaining the integrity of the flows). In a controlled network Net Optics offers the Indigo Pro management platform to centralize the management of many of its installed products.

4. DISCUSSION

Controlling virtualized environments In recent years, there has been a widespread popularization of virtualized network environments that increase the efficiency and flexibility of IT (information technology) systems, as well as reduce costs. However, in the same hypervisor itself, it is not possible to capture and analyze the traffic transmitted between virtual machines with the help of conventional physical monitoring tools. Lack of control over this traffic poses a threat to the information security of the enterprise and makes it difficult to detect (diagnose) network outages. As a solution to this problem, Net Optics offers the use of its own Phantom Virtualization Tap (DT) software designed to control traffic in virtualized computing environments. The Phantom Monitor component, which is installed inside the hypervisor core of this software solution, captures (captures) all traffic transmitted between virtual machines via a virtual switch (switch) and captures captured (captured) packets. mental filtering, as well as sending the data to be monitored. In addition, this component has the ability to send captured (captured) traffic to a physical network port for monitoring using traditional physical monitoring tools. The Phantom Virtualization Tap solution does not interfere with the operation of virtual machines and does not require any modification (change of appearance). The second major software component of this solution, the Phantom Manager, is designed to collect and transmit traffic information, as well as to manage a large number of virtual networkers running on controlled hosts. Statistics on the performance of virtual environments are provided in the second and third stages (number of packets transmitted, loading, etc.). Of course, to monitor the virtualized environment, it is possible to extract traffic from it with the help of SPAN-ports of the virtual connector, but for this purpose up to half of the capacity of this connector is spent. In contrast, the Phantom Virtualization Tap virtual network does not load the virtual connector, and its bandwidth remains unchanged. Phantom Virtualization Tap solution for the most common virtualization tools (platforms): VMware vSphere ESX / ESXi Server 4.x / 5.x; Microsoft Hyper-V 8.x; Citrix Xen Server 5.6.x; Redhat KVM 2.6.32 and Oracle VM 3.0 compatible (compatible). This solution helps to ensure the security and reliability of virtual environments, as well as their compliance with regulatory requirements. It is necessary to prepare for monitoring in advance

5. CONCLUSION

Optimal connection Monitoring the operation of a network and network services and applications involves capturing and analyzing network traffic. This is not only to identify (diagnose) problems in the network, but also to optimize the work of critical services and applications, as well as information security within the framework of the System of Technical Means (SORM) to ensure the functions of operational search activities. in order to identify relevant threats and to legally intercept (capture) information transmitted over the network. IT specialists record various volumes of monitoring tools, including protocol analyzers, RMON tubing devices (probes), NetFlow collectors (collectors), IDS / IPS systems, and large amounts of network traffic. use test tools (probes) based on available server platforms (see section "Analysis, monitoring and detection (diagnostics) of the corporate network"). In order to capture the network traffic that needs to be controlled, it is preferable to use a special network of monitoring devices (a device that divides the network into branches) or disconnectors (switches) that have the functions of such a network to connect them to the network.

6. REFERENCES

1. Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.
2. Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.
3. Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.
4. Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.
5. Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.
6. Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.
7. Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013
8. Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013
9. Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013
10. Explanatory dictionary of information and communication technologies (second edition). - T., 2010.